Intelligent Network-Based Early Warning Systems

Karsten Bsufka, Olaf Kroll-Peters, and Sahin Albayrak

Technische Universität Berlin, DAI-Labor
{karsten.bsufka,olaf.kroll-peters,sahin.albayrak}@dai-labor.de

Abstract. In this paper we present an approach for an agent-based early warning system (A-EWS) for critical infrastructures. In our approach we combine existing security infrastructures, e.g. firewalls or intrusion detection systems, with new detection approaches to create a global view and to determine the current threat state.

Keywords: critical infrastructures, early warning system, multi agent systems, intrusion detection.

1 Introduction

Modern societies depend heavily on certain infrastructures, which are critical for existence and smooth operation of society. Examples for these critical infrastructures are:

- Transportation and traffic
- Telecommunications and information technology
- Finance and insurance services
- Supplies
  - Health care
  - Emergency services
  - Water supply
  - Energy supply
- Public administration and legal system [2]

With the dawning information age these infrastructures lose the independent character. The main reason for this loss of independence lies within the emergence of information technology infrastructures and the Internet.

Every critical infrastructure is based on its underlying networks. These separate networks are connected by Internet provider networks, see Figure 1.

Figure 1 is similar to a figure presented in [5], which shows how *bounded* networks reside within an *unbounded* domain. Generally speaking bounded networks are under single administrative control and adhere to known security policies. Unbounded networks on the other hand are under different administrative controls and there is no global visibility of the network. As a consequence, problems

J. Lopez (Ed.): CRITIS 2006, LNCS 4347, pp. 103–111, 2006.

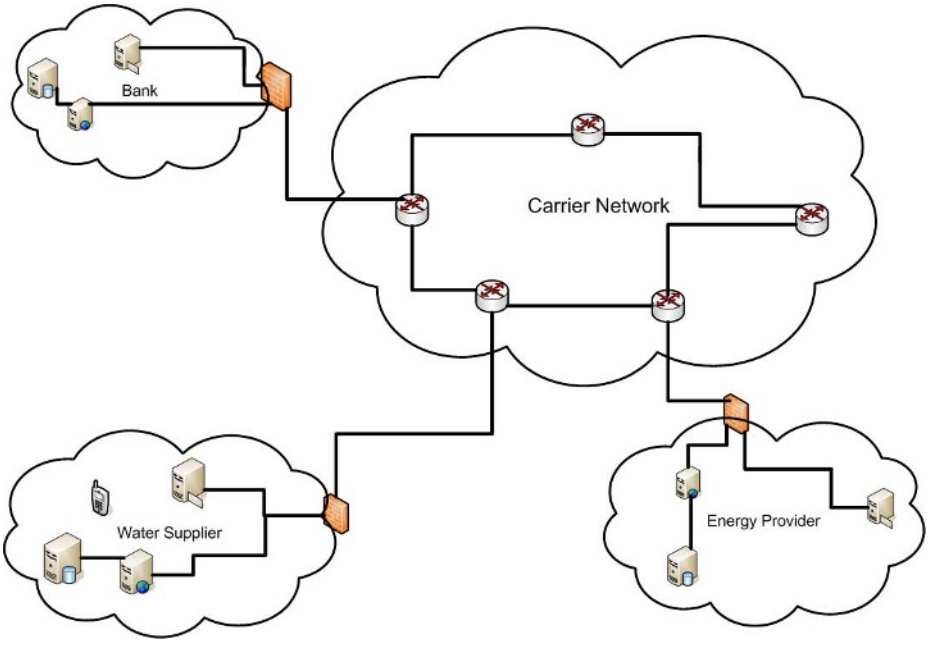

Fig. 1. Overview of CRITIS networks

occurring within one critical infrastructure, e.g. power failures caused by natural disasters or attacks are carried out against transport systems, will not be communicated to other critical infrastructures.

We propose an early warning system for critical infrastructures, which helps to relay information about threatened critical infrastructures. Before we go into details about our proposed agent-based early warning system for critical infrastructures, we first describe some potential scenarios for a breakdown of critical infrastructures, the role of IT systems and the potential effects in these situations.

2 Breakdown Scenarios for Critical Infrastructures

There are several potential causes for a breakdown or limited availability of a critical infrastructure. Obvious causes would be attacks (cyber or physical) or natural disasters, other reasons may include (labor) strikes, erroneous use or technical failures of IT systems or other systems. A detailed discussion of critical infrastructures can be found in [9].

The threats to critical infrastructures can be classified into the following different categories.

- Financial threats
- Material threats